C1415

#4

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 782 114 A2

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
02.07.1997 Bulletin 1997/27

(51) Int. Cl.[6]: **G07C 9/00**

(21) Application number: **96308730.9**

(22) Date of filing: **03.12.1996**

(84) Designated Contracting States:
DE FR GB

(30) Priority: **29.12.1995 US 586020**

(71) Applicant: **International Business Machines Corporation**
Armonk, N.Y. 10504 (US)

(72) Inventors:
- **Dwork, Cynthia**
  Palo Alto, California 94301 (US)
- **Naor, Moni**
  Tel Aviv, 69122 (IL)
- **Pestoni, Florian**
  Buenos Aires, 1426 (AR)

(74) Representative: **Bailey, Geoffrey Alan**
IBM United Kingdom Limited
Intellectual Property Department
Hursley Park
Winchester Hampshire SO21 2JN (GB)

(54) System and method for verifying signatures on documents

(57) A system and method are provided for producing verified signatures on documents such as checks and affidavits. Initially, a customer who is to obtain a verified signature, at some point in time, registers with a signatory authority, and a secret key, having public and private components, is established uniquely for that customer. When a document requires a verified signature, the customer presents the document and proof of his/her identity, such as a preprogrammed computer-interfacable card, to a signature system. Typically, such a system is to be available at an institution, such as an office, bank, or post office, where such services will routinely be used. The system accesses the archive of the private portion of the customer's key, and generates an encoded signature based, in part, on the content of the document. Accordingly, when a recipient of the document later wishes to verify the signature, the recipient uses the customer's public key to decode the signature. It is then straightforward to verify the signature against the content of the document.

EP 0 782 114 A2

While the invention is primarily disclosed as a method, it will be understood by a person of ordinary skill in the art that an apparatus, such as a conventional data processor, including a CPU, memory, I/O, program storage, a connecting bus, and other appropriate components, could be programmed or otherwise designed to facilitate the practice of the method of the invention. Such a processor would include appropriate program means for executing the method of the invention.

Also, an article of manufacture, such as a pre-recorded disk or other similar computer program product, for use with a data processing system, could include a storage medium and program means recorded thereon for directing the data processing system to facilitate the practice of the method of the invention. It will be understood that such apparatus and articles of manufacture also fall within the scope of the claims.

Brief Description of the Drawings

FIG. 1 is a high-level flowchart showing the method of the invention.

FIG. 2 is a flowchart showing a more detailed implementation of a step of the flowchart of FIG. 1.

FIG. 3 is a flowchart showing a more detailed implementation of a step of the flowchart of FIG. 1.

FIG. 4 is a block diagram of a system for practising the method of the invention.

Description of the Preferred Embodiment

In accordance with the invention, a signature is generated for a document, using a secret key. The secret key is preferably implemented as per the well-known public/private key system of RSA Data Security, which is well-known in the field of cryptography. In such a system, a given customer is assigned a unique secret key, having a public key and a private key component.

It is a characteristic of the key components that, if either one is used to encrypt a plaintext message, the other decodes the encrypted message. Further, given the public key component, it is computationally infeasible to generate the private key component.

Therefore, a sender can encrypt a message intended only for the eyes of a recipient, using a recipient's public key, and send the encrypted message, knowing that only the recipient has the private key necessary to decrypt the message. On the other hand, a sender can encrypt a message using the sender's private key, so that any recipient who decrypts the message using the sender's public key knows that the message must have originated from the sender, because only the sender has the sender's private key.

The method of the invention takes advantage of the workings of such a scheme, by using the latter characteristic, to establish with certainty that the signature is that of the sender, or of a sender's authorized agent.

FIG. 1 is a high level flowchart of the method of the invention. Separate steps, which form novel and non-obvious aspects of the invention, take place at different times. The steps shown in FIG. 1 are grouped, based on times at which the steps preferably take place.

Initially, step 2 of the method includes establishing and maintaining a secret key, such as the public/private key referred to above, associated with a respective customer, who is to provide a document requiring a signature. Preferably, a database of such keys is established, each customer having a public key, available to any interested party, and a private key, known only to the customer. The private key is archived in a suitably secure way, and the public key is made available to the public.

A preferred format for the public key is a two-dimensional code signed with a system key which is maintained by the system, and over which an authorized system administrator has control.

Also, a customer can request that his/her key be notarized. This is preferably done as follows: the customer presents the two-dimensional code signed with the system key, and proof of the customer's identity, to an authority. The authority then produces a two-dimensional encoding of the key presented, signed with the private key of the authority.

It is expected that, in typical, preferred implementations of the invention, step 2 takes place as a customer registers for services provided by the invention, possibly before the customer has a document for which he/she requires a verified signature.

When such a database is in place, a customer provides a document for a signature (step 4). Step 3 of FIG. 1, which collectively incorporates steps 4, 6, and 8, shows the activities associated with generating the signature.

In step 6, a digital signature is generated for the document, using the customer's secret key. Preferably the private key component of the customer's secret key is used. Also, the signature is preferably generated using, as input information, data pertaining to the document itself, such as a scanned bit map of the document. Therefore, the signature produced by step 6 is unique to the customer by virtue of its use of the customer's private key, as well as being unique to the document, by virtue of being based on the content of the document. Accordingly, the signature is demonstrably authentic with regard to both the document and the customer.

A preferred implementation of step 6, given in FIG. 2, includes producing a two-dimensional encoding of the content of the document, as well as the signature (step 20). The appropriate authority responds with a receipt in the form of a hash of the information presented, signed with the private key of the authority (step 22). Accordingly, no further proof of the customer's identity needs to be shown. Thus, forms can be sent by mail.

It is understood, also, that a signatory authority, such as a notary public or other suitable official, can also produce a signature as described above. Such a

embodiments may occur to one skilled in the art without departing from the scope of the present invention as set forth in the following claims.

Claims

1. A signature verification method for use with a document which is to bear a signature by a customer, the method being characterised by the steps of:

   maintaining a database (2) of keys associated with respective parties, including the customer, who are to make signatures that are to be verified using the signature verification method of the invention, each of the keys including a securely archived private key and a publically available public key,

   generating a digital signature (6), employing the customer's private key; the signature being based on the content of the document;

   associating the signature (8) with the document;

   decoding the signature (10) based on the customer's public key, thereby verifying that the customer signed the document because the customer's private key was used; and

   verifying the content (12) of the document against the decoded signature, thereby verifying that the signature was made for the document.

2. A signature verification method as recited in claim 1, wherein the step of maintaining a database of keys includes the steps of:

   generating a key; and

   notarizing the key.

3. A signature verification method as recited in claim 1 or 2, wherein:

   (i) the step of maintaining a database of keys includes the steps, executed for a customer, of:

      generating a key pair including a private key and a public key, storing the private key in a secure way, and
      outputting the public key as a two-dimensional code; and

   (ii) the step of notarizing includes the steps of:

      presenting the two-dimensional code and proof of the customer's identity to an authority, the authority having a private key,

      generating a two-dimensional encoding (20) of the key presented, the encoding including a signature of the private key of the authority, and

      presenting the two-dimensional encoding (22) of the key presented, signed with the private key of the authority, as a receipt to the customer.

4. A signature verification method as recited in claim 3, wherein the said two-dimensional code of the public key is signed using a predetermined system key.

5. A signature verification method as recited in any previous claims wherein the step of generating a digital signature includes establishing the customer's identity (32).

6. A signature verification method as recited in claim 5, wherein:

   the step of maintaining a database of keys includes issuing the customer an identity card programmed with information regarding the customer's identity; and

   the step of establishing the customer's identity includes:

      (i) establishing an interface (30) between the identity card and a signature system having an identity card interface and a user interface, and

      (ii) the user interactively performing an identification procedure (32), using the user interface, wherein the user's identity is established based on the programming of the identity card.

7. Apparatus comprising a data processor including a CPU and memory and including stored program control designed to execute the method as claimed in any previous claim.

8. A data storage medium having program means recorded thereon and designed to direct a data processing system to execute the method as claimed in any one of claims 1 to 6.

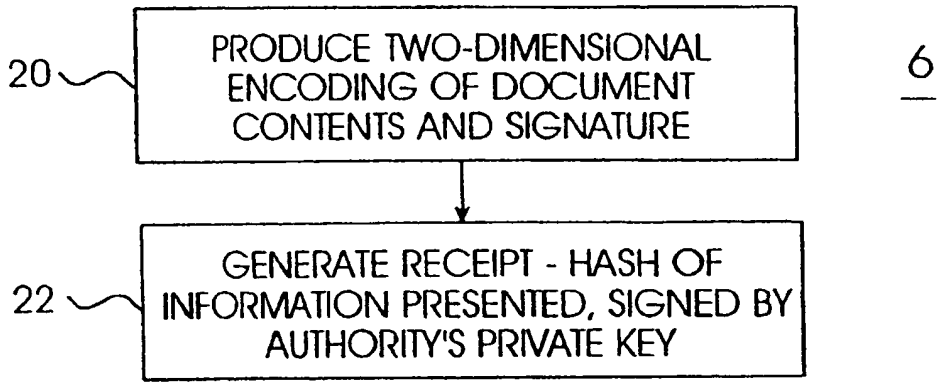
20
PRODUCE TWO-DIMENSIONAL ENCODING OF DOCUMENT CONTENTS AND SIGNATURE
6
22
GENERATE RECEIPT - HASH OF INFORMATION PRESENTED, SIGNED BY AUTHORITY'S PRIVATE KEY

FIG. 2

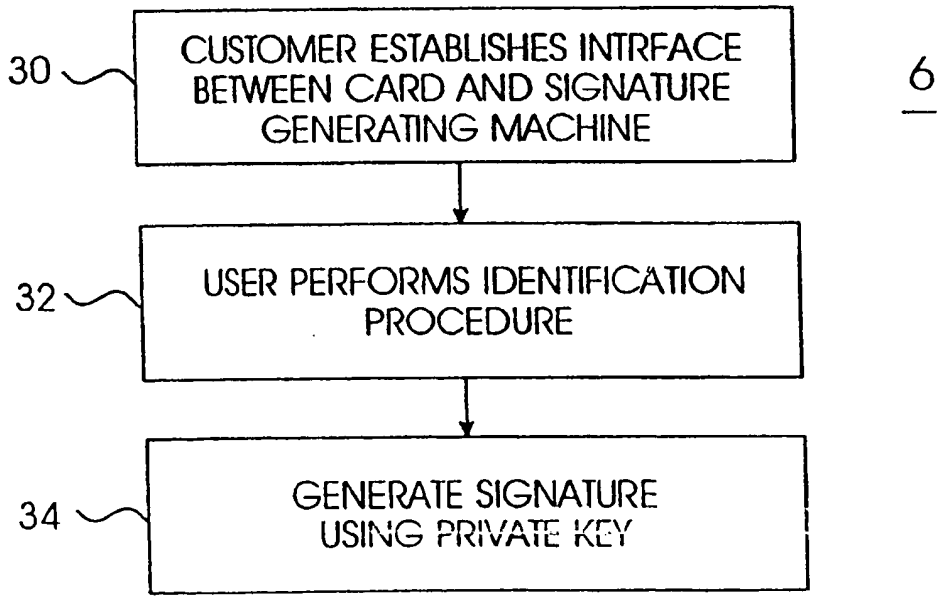
30
CUSTOMER ESTABLISHES INTRFACE BETWEEN CARD AND SIGNATURE GENERATING MACHINE
6
32
USER PERFORMS IDENTIFICATION PROCEDURE
34
GENERATE SIGNATURE USING PRIVATE KEY

FIG. 3

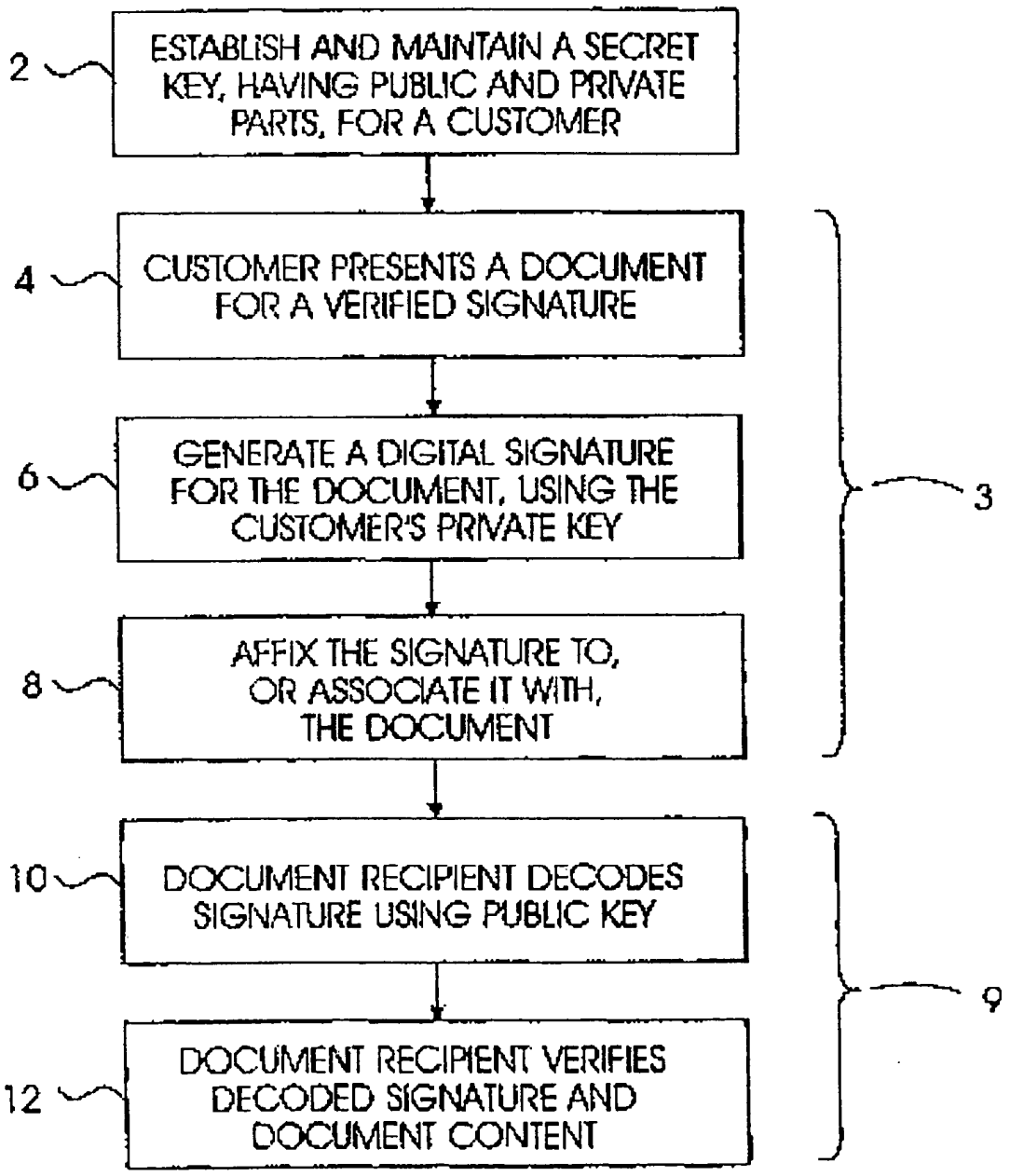
2
ESTABLISH AND MAINTAIN A SECRET KEY, HAVING PUBLIC AND PRIVATE PARTS, FOR A CUSTOMER
4
CUSTOMER PRESENTS A DOCUMENT FOR A VERIFIED SIGNATURE
6
GENERATE A DIGITAL SIGNATURE FOR THE DOCUMENT, USING THE CUSTOMER'S PRIVATE KEY
8
AFFIX THE SIGNATURE TO, OR ASSOCIATE IT WITH, THE DOCUMENT
3
10
DOCUMENT RECIPIENT DECODES SIGNATURE USING PUBLIC KEY
12
DOCUMENT RECIPIENT VERIFIES DECODED SIGNATURE AND DOCUMENT CONTENT
9

FIG. 1

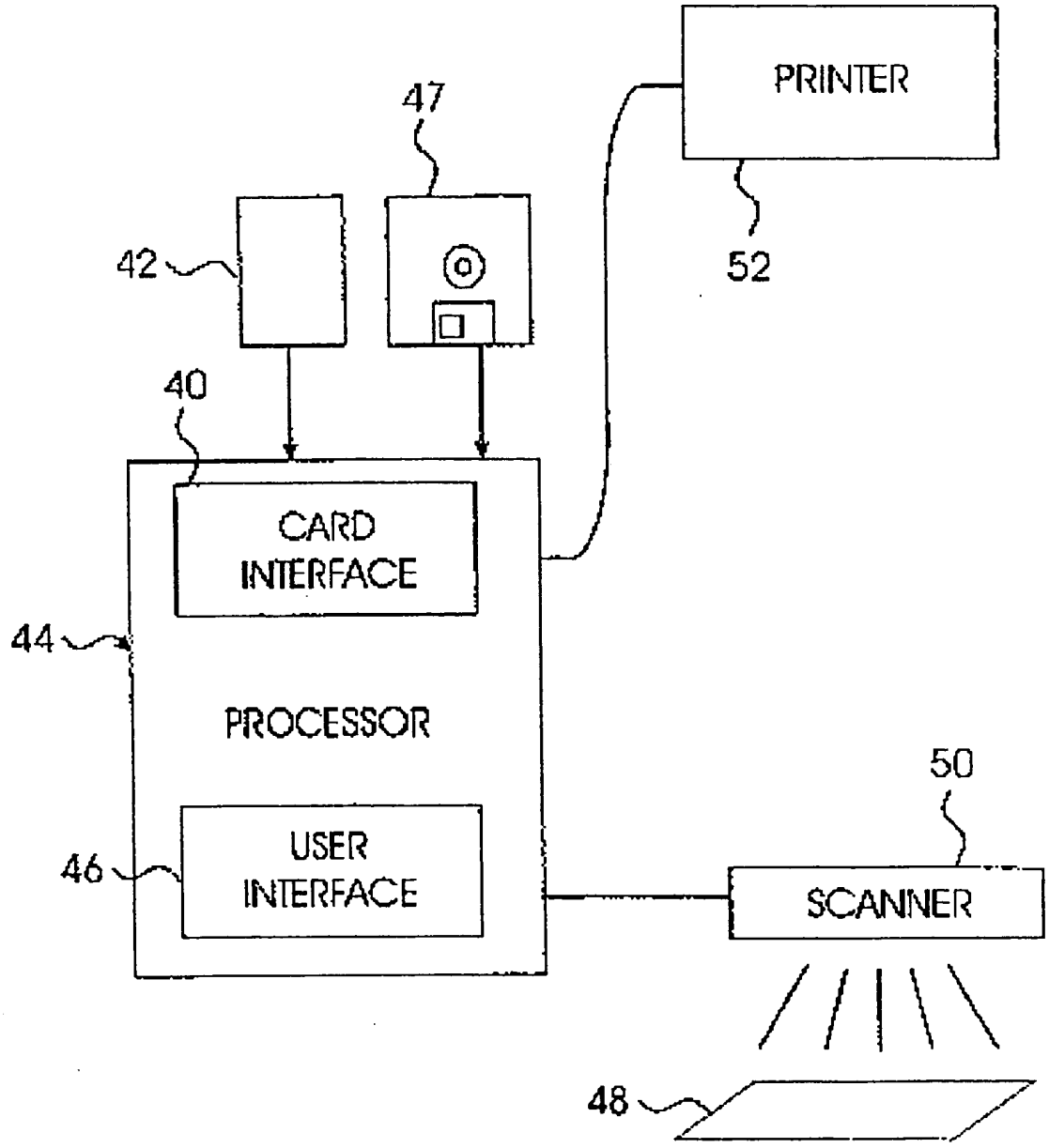
PRINTER
47
52
42
40
CARD
INTERFACE
44
PROCESSOR
50
46
USER
INTERFACE
SCANNER
48

FIG. 4